CHAPTER 5

Wireless LAN Example Scenario

The wireless LAN relies on high-speed wireless *hot spots*. Unlike public hot spots —which have begun to appear in airports, hotel lobbies, and coffee shops, allowing anyone with a wireless-enabled computer or PDA to access the Internet—the hot spots used by police, firefighters, and paramedics are secure and accessible only to authorized personnel.

High-speed wireless LANs can send and receive live video feeds, known as IP video. This technology can be used to monitor public areas from remote locations and to gain insight into rapidly developing or escalating situations. Incident commanders can view structure fires, protests, and other events as they’re happening, helping them to direct response teams and resources accordingly.

A 911 dispatcher can send a police helicopter to the scene of a fire, giving emergency services personnel a better idea of the resources needed to control the situation, to save lives, save property, and gather evidence. It also helps various agencies coordinate resources.

On the ground, ambulances can transmit live video and data, allowing medical teams to observe the condition of patients before they arrive. Police can monitor areas of concern without actually driving there, preserving the safety of emergency personnel. Officers can view fellow officers as they make traffic stops and respond to disturbances, instead of simply retrieving videotape from a cruiser after something has gone wrong.

High-speed wireless LAN coverage can be limited to one or two hot spots measuring a few hundred feet in diameter, or a wireless LAN can be extended across an entire community by using multiple overlapping hot spots.

802.11 wireless technology is attractive to many municapalities because deployment can begin with the establishment of hot spots around police stations and firehouses, and expanded to other areas as resources become available and utilization increases.

At the center of each hot spot is a devices known as an access points, which can be connected to a wired or a wireless network to create secure wireless gateways, enabling authorized personnel to send and receive data using wireless-enabled notebooks, PDAs, and other devices. And 802.11 wireless technology is now portable as a result of recent developments at Cisco Systems, Inc.

A vehicle can be equipped with a router, a bridge, and an access point. The bridge provides wireless communications with the municipal LAN. The access point communicates with devices that would otherwise be out of range of a fixed hot spot. The router manages fast, reliable communications between the local devices and the municipal LAN.

Silicon Beach Police Example Scenario

The mission is for Silicon Beach Police to extend its mobility, increase work efficiency, and improve the quality of its services to the public.

Until recently, when police respond to a robbery, they have no idea what to expect when they get there. This lack of information is a major disadvantage. However, with an IP video surveillance solution, that is no longer the case. When an alarm is triggered at the scene of a robbery, the existing security cameras transmit the video over a network of wireless routers, bridges, and access points.

Police officers can see what is happening inside the bank from any wireless hot spot. Emergency vehicles can become mobile wireless hot spots, maintaining high-speed connections while in motion, allowing officers to make faster, better, safer decisions.

Without this technology, police must rely on witnesses, limited observations made from outside the building, and voice descriptions. With this technology, police can see inside a building in real time. As a result, the incident is more likely to be brought to a conclusion with a minimum risk of injury, loss of life, or loss of property.

Without this technology, a suspect is typically transported to headquarters to be photographed and fingerprinted by police technicians, who must manually compare the results to relevant databases. A wireless LAN in the officer’s cruiser connected to the municipal LAN enables the officer to conduct a real-time database query on the suspect, verifying the suspect’s identity, but could lead to a match with information from an unsolved case.

Objective

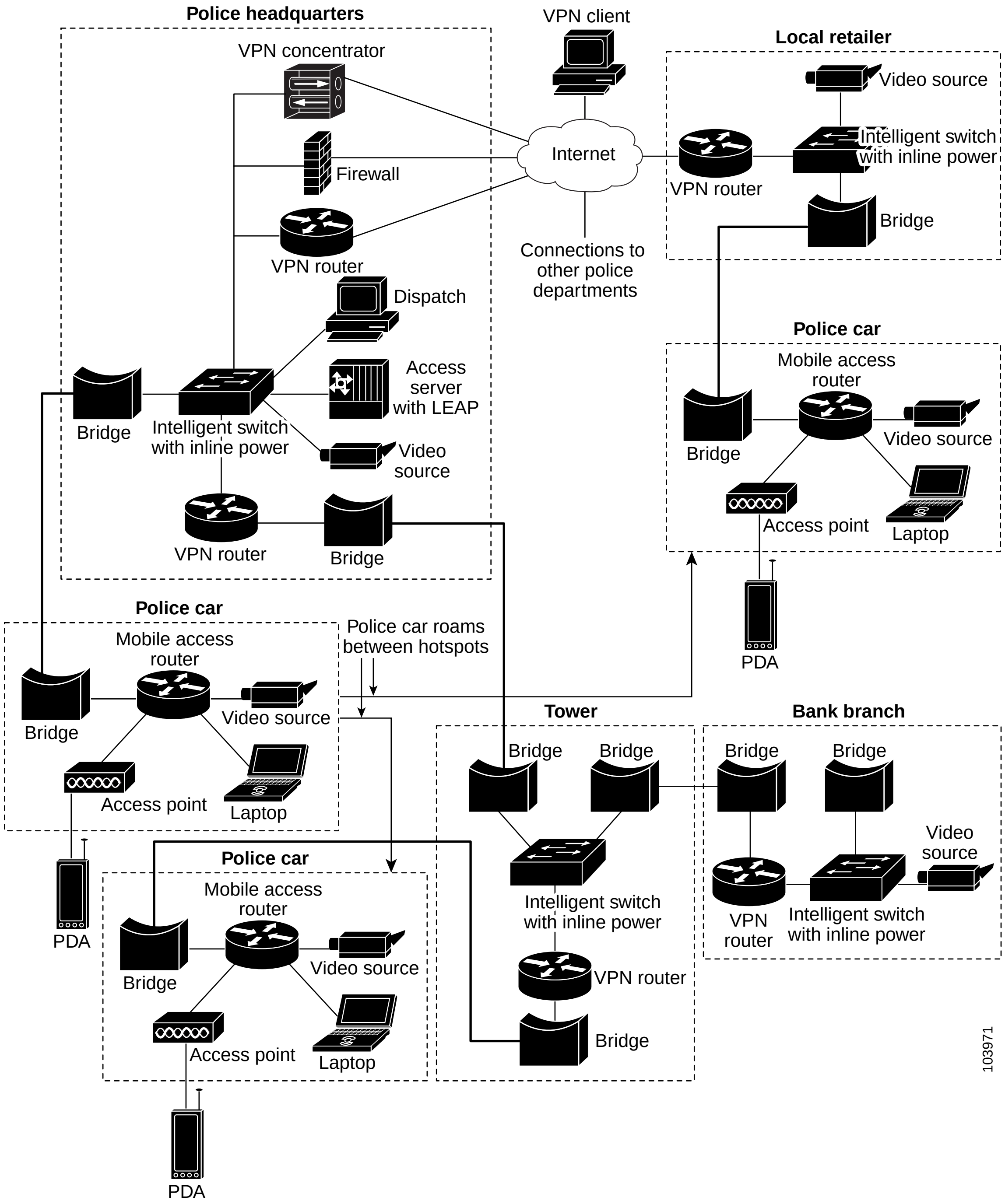
To provide a mobile wireless solution that enables Silicon Beach Police to obtain a seamless, continuous network connections with other wireless and wired network services. The recommended solution meets the following requirements:

- Seamless, continuous wireless connections from the police vehicle to the home network.
- Streaming real-time video across the network, including headquarters and other police vehicles.
- End to end security

Approach

Create Mobile IP hotspots that allow the router to connect to the home network while the emergency vehicles are mobile. Figure 5-1 shows the Cisco Mobile IP home network at police headquarters, and foreign agent hotspots.

Figure 5-1 Configuration Overview



There are four hotspots:

- police department headquarters
- bank
- retail establishment
- traffic light, used as a tower

Silicon Beach Police includes a secure connection to other emergency services, such as the fire department, through the Internet by using a VPN tunnel. Each hotspot contains an Access Point that communicates with the wireless workgroup bridge inside the police vehicles to provide network connectivity to these police vehicles. The setup includes:

- Video cameras mounted at the bank and police stations
- Video servers that can record and archive
- Alarm Triggered Internet Protocol

Silicon Beach Police Officers in properly equipped cruisers can view real-time video of a crime scene on their laptops as soon as an alarm is triggered, and respond according to what they see occurring. The video feeds are also accessible on Personal Digital Assistants (PDAs), providing even greater intelligence gathering flexibility.

A camera mounted on the dashboard of the police cruiser is connected to the municipal LAN. The live image can be viewed by authorized personnel from anywhere in the Silicon Beach Police network, including headquarters, a mobile command center, or other police vehicles.

Security is implemented in two forms: VPN and LEAP. VPN tunnels secure the data in both the wired and wireless networks. Security between a cruiser and a foreign agent, such as the bank, is supported by the wireless device. LEAP authenticate devices to an ACS server in the home network. When a client, such as a personal computer, associates with the access point on the cruiser, the personal computer is authenticated before any traffic is allowed through the access point.

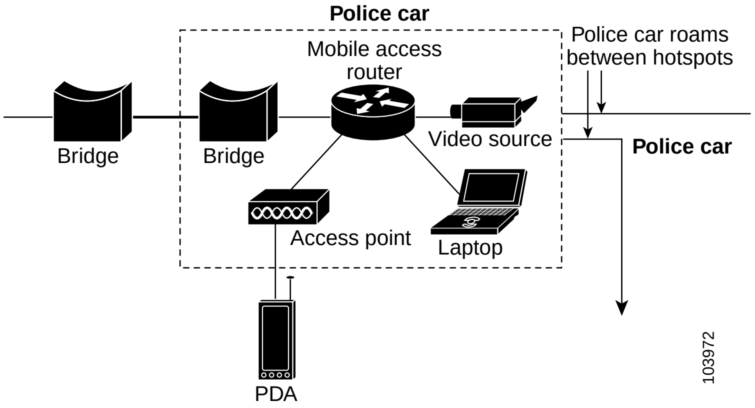
Patrol Car Example Configurations

The hardware and software components in each mobile police unit include:

- One Cisco 3220 Series Mobile Access Router with two Cisco 3201 Wireless Mobile Interface Cards, one configured to be an access point and the other as a wireless workgroup bridge.
- One analog camera
- One video server (IP out)
- A laptop personal computer with viewing software

Figure 5-2 shows the police car configuration. Note that the wireless workgroup bridge and the access point are attached to and draw power from the router.

Figure 5-2 Patrol Car Configuration



The bridge links the cruiser mobile access router to the larger municipal LAN. The bridge and the access point connect to the router through internal Ethernet connections. The router can be connected to the remaining LAN devices by using wireless connections, Ethernet ports, or serial ports. Depending on the configuration, the access point could associate with devices in other vehicles.

Police Cruiser Cisco 3200 Mobile Access Router Configuration Example

The Ethernet port on each WMIC is connected to Ethernet ports on the FastEthernet switch card or the Ethernet port on one WMIC might be connected to the Ethernet port on the mobile access router card. We recommend that the WMIC Ethernet ports be connected to the FastEthernet switch card. However, your configuration might be different, depending on how your system integrator assembled the router.

Typically these connections are made internally. These links provide communications between the WMICs and the router. It is not necessary to make a similar connection between the FastEthernet switch card and the mobile access router card, because the FastEthernet switch card communicates with the mobile access router card through the bus.

```
no spanning-tree vlan 1
!
ip dhcp excluded-address 192.168.100.5
ip dhcp excluded-address 192.168.100.1
!
ip dhcp pool MobileNetwork
  network 192.168.100.0 255.255.255.0
  default-router 192.168.100.1
!
crypto isakmp policy 1
 hash md5
 authentication pre-share
 group 2
crypto isakmp key 1234567890 address 60.1.1.2
!
crypto isakmp peer address 60.1.1.2
!
crypto ipsec transform-set testtrans ah-md5-hmac esp-aes 256 esp-sha-hmac comp-lzs
!
crypto map ToSecureNet 10 ipsec-isakmp
 set peer 60.1.1.2
 set transform-set testtrans
 match address 155
```

```
!
interface Loopback1
 ip address 66.1.1.5 255.255.255.0
 crypto map ToSecureNet
!
interface FastEthernet0/0
 ip address 192.168.100.1 255.255.255.0
 ip policy route-map SecureNetPolicy
 description Connection_to_Access_Point
 duplex auto
 speed auto
!
interface FastEthernet2/0
 no ip address
 shutdown
!
interface FastEthernet2/1
 no ip address
 shutdown
!
interface FastEthernet2/2
 no ip address
 shutdown
!
interface FastEthernet2/3
 descriptiong WMIC_WGB_Connection
 no ip address
!
interface Vlan1
 ip address 70.70.70.2 255.255.255.0
 ip mobile router-service roam priority 255
 ip mobile router-service solicit interval 1
!
ip local policy route-map SecureNetPolicy
!
access-list 155 permit ip 192.168.100.0 0.0.0.255 any
!
route-map SecureNetPolicy permit 10
 match ip address 155
 set interface Loopback1
!
router mobile
!
ip mobile secure home-agent 200.200.200.1 spi 100 key hex 12345678123456781234567812345678
algorithm md5 mode prefix-suffix
!
ip mobile router
  address 65.1.1.5 255.255.255.0
  home-agent 200.200.200.1
  reverse-tunnel
```

Police Cruiser Wireless Workgroup Bridge Configuration Example

One Ethernet port on the WMIC connects the card configured as a workgroup bridge to an Ethernet port on either the FastEthernet switch card or the mobile access router card. Typically this connection is made internally, and provides communications between the WMIC being used as a workgroup bridge and the router.

If the connection is made to the FastEthernet switch card, is not necessary to connect the FastEthernet switch card to the mobile access router card by using the FastEthernet ports, because the FastEthernet switch card communicates with the mobile access router card through the bus.

```
bridge irb
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption key 1 size 128bit 0 12345678901234567890123456 transmit-key
 encryption mode wep mandatory
 !
 ssid silicon_beach_hotspot
    infrastructure-ssid
 !
 cca 0
 concatenation
 speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
 rts threshold 4000
 power local cck maxmimum
 power local ofdm maximum
 power client maximum
 station-role workgroup-bridge
 mobile station
 infrastructure-client
 bridge-group 1
 bridge-group 1 spanning-disabled
!
interface FastEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 bridge-group 1 spanning-disabled
!
interface BVI1
 ip address dhcp
 no ip route-cache
!
ip radius source-interface BVI1
bridge 1 route ip
```

Police Car Access Point Configuration Example

One Ethernet port on the WMIC connects the card configured as an access point to an Ethernet port on either the FastEthernet switch card or the mobile access router card. Typically this connection is made internally. This link provides communications between the WMIC being used as an access point and the router.

If the connection is made to the FastEthernet switch card, is not necessary to connect the FastEthernet switch card to the mobile access router card by using the FastEthernet ports, because the FastEthernet switch card communicates with the mobile access router card through the bus.

```
bridge irb
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption key 2 size 128bit 0 12345678901234567890123456 transmit-key
 encryption mode wep mandatory
 !
 ssid silicon_beach_wep
    authentication open
    infrastructure-ssid
 !
 cca 0
 concatenation
 speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
 rts threshold 4000
 power local cck maximum
 power local ofdm maximum
 power client maximum
 channel least-congested
 station-role root ap-only
 infrastructure-client
 bridge-group 1
 bridge-group 1 spanning-disabled
!
interface FastEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 bridge-group 1 spanning-disabled
!
interface BVI1
 ip address 192.168.100.5 255.255.255.0
 no ip route-cache
!
ip default-gateway 192.168.100.1
!
ip radius source-interface BVI1
bridge 1 route ip
```